Statement of Chairman Tom Davis
Government Reform Committee Hearing,
"Once More Into the Data Breach:
The Security of Personal Information at Federal Agencies"
June 8, 2006

Secure information is the lifeblood of effective government policy and management, yet federal agencies continue to hemorrhage vital data. Recent losses of critical electronic records compel us to ask: What is being done to protect the sensitive digital identities of millions of Americans, and how can we limit the damage when personal data does go astray?

In early May, a Department of Veterans Affairs employee reported the theft of computer equipment from his home, equipment that stored more than 26 million records containing personal information. While he was authorized to access those records, he was not part of any formal telework program.

VA leadership delayed acting on the report for almost two weeks, while millions were at risk of serious harm from identity theft. And since admitting to the largest data loss by a federal agency to date, the VA has been struggling to determine the exact extent of the breach. Just yesterday, we learned the lost data includes information on over 2 million active duty and reserve personnel, as well as veterans. So the security of those currently serving in the military may have been compromised, and the bond of trust owed to those who served has been broken.

And that is only the latest in a long string of personal information breaches in the public and private sectors, including financial institutions, data brokerage companies, and academic institutions. Just recently, a laptop computer containing information on nearly 300 Internal Revenue Service employees and job applicants – including data such as fingerprints, names, Social Security numbers, and dates of birth – was lost while in transit on an airline flight, according to reports.

These breaches illustrate how far we have to go to reach the goal of strong, uniform, government-wide information security policies and procedures.

On this Committee, we've been focused on government-wide information management and security for a long time. The Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. These incidents highlight the importance of establishing – and following -- security standards for safeguarding personal information. They also highlight the need for pro-active security breach notification requirements for organizations -- including federal agencies -- that deal with sensitive personal information.

I know other Committees have been working on requirements for the private sector. Federal agencies present unique requirements and challenges, and it is my hope

that we can work to strengthen personal data protections through regulatory changes, and any needed legislative fixes.

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to provide protections for agency data and information systems to assure their integrity, confidentiality, and availability. FISMA requires each agency to create a comprehensive risk-based approach to agency-wide information security management. It is intended, in part, to make security management an integral part of everyday operations.

Some complain that FISMA is little more than a paperwork exercise, an analog answer to a digital problem. This latest incident disproves that complaint. FISMA requires agencies to notify agency Inspectors General and law enforcement, among others, when a breach occurs. It appears VA has not complied with that requirement.

Each year, the Committee releases scorecards based on the information provided by Chief Information Officers and Inspectors General in their FISMA reports. This year the scores for many departments remained unacceptably low or dropped precipitously.

The Veterans Affairs Department earned an F, the second consecutive year and fourth time in the past five years the department receiving a failing grade. The federal government overall received a D+, although several agencies improved their information security or maintained a consistently high level of security from previous years, including the Social Security Administration.

Today, the Committee wants to discuss how we can improve the security of personal information held or controlled by federal agencies. In my view, these efforts should include strengthening FISMA, and adding penalties, incentives, or pro-active notification requirements.

The Office of Management and Budget will discuss government-wide efforts to improve data security. GAO will highlight areas in which the protection of consumer information can be enhanced. In this context, we'll focus on security at Veterans Affairs, the Social Security Administration, and the IRS. VA Secretary Nicholson will discuss the details of that department's potentially catastrophic data breach. Officials from the IRS and the Social Security Administration will describe the experiences and efforts of those agencies, which stand as guardians of the largest storehouses of taxpayer information.

Government information systems hold personal information about millions of citizens, including health records, military service histories, tax returns, and retirement accounts. E-commerce, information sharing, on-line tax filing, are commonplace. If the federal government is going to be a trusted traveler on the information superhighway, critical data on millions of citizens should not be able to go missing after a trip on the Beltway in the back seat of a federal employee's car.